



DAF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

IAN M. DRYSDALE

Serial No.: 09/466,271

Filed: December 17, 1999

For: METHOD AND DEVICE FOR PERFORMING CARD TRANSACTIONS

Attorney Docket No.: FDC 0135 PUS (012200US)

Group Art Unit: 3693

Examiner: Borlinghaus, Jason M.

REPLY BRIEF UNDER 37 C.F.R. § 41.41

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
U.S. Patent & Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This Reply Brief is in response to the Examiner's Answer mailed April 5, 2007, for the above-identified patent application. The Examiner's Answer is in response to the Applicant's Appeal Brief mailed January 2, 2007.

The Examiner's Answer did not contain a new ground of rejection. The Applicant requests the appeal be maintained and wishes to file this Reply Brief to address the Examiner's Answer.

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8 (FIRST CLASS MAIL)		
I hereby certify that this paper, including all enclosures referred to herein, is being deposited with the United States Postal Service as first-class mail, postage pre-paid, in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, U.S. Patent & Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 on:		
<u>May 14, 2007</u> Date of Deposit	<u>James N. Kallis</u> Name of Person Signing	<u>[Signature]</u> Signature

## **Applicant's Reply to (10) Examiner's Response to Argument**

### **1. The Independent Claims**

The Applicant's independent claims 1 and 11-12 generally include:

(i) the merchant service provider ("MSP") web server has commands for processing transaction information associated with the transaction card to obtain authorization from the MSP for the transaction;

(ii) the transaction device (terminal) does not use any MSP proprietary software for the transaction information to be processed to obtain authorization from the MSP for the transaction; and

(iii) the transaction device (terminal) accesses the web server without accessing any MSP proprietary network.

### **2. Piecemeal Examination**

The Examiner cited *Muftic*, *PR Newswire*, and *Booker* for respectively teaching the claimed items (i), (ii), and (iii). In the Appeal Brief, the Applicant argued *Muftic*, *PR Newswire*, and *Booker* respectively do not teach or suggest the claimed items (i), (ii), and (iii). In the Examiner's Answer (page 11), the Examiner indicated the Applicant and the Board should refrain from conducting piece-meal analysis of prior art references, as "one cannot show non-obviousness by attacking references individually where, as here the rejections are based on combinations of references." *In re Keller, Terry, and Davies*, 208 USPQ 871, 882 (CCPA 1981). To this end, the Examiner noted the Applicant refuted *Muftic*, *PR Newswire*, and *Booker* individually, rather than viewing them in combination, in light of the totality of their combined teachings.

The Applicant notes all the claimed items (i), (ii), and (iii) must be taught or suggested by the prior art. As indicated in MPEP § 2143.03, "To establish *prima facie*

obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art.” *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). In the Appeal Brief, the Applicant argued none of *Muftic*, *PR Newswire*, and *Booker* respectively teach or suggest the claimed items (i), (ii), and (iii). Thus, the combination of *Muftic*, *PR Newswire*, and *Booker* as posited by the Examiner does not teach or suggest all the claim limitations recited in independent claims 1 and 11-12. As such, “viewing [*Muftic*, *PR Newswire*, and *Booker*] in combination, in light of the totality of their combined teachings” does not result in a combination which teaches or suggests all the claim limitations recited in independent claims 1 and 11-12.

### 3. Claimed Item (i) Compared to *Muftic*

The Applicant again addresses the Examiner’s position that *Muftic* discloses the claimed item (i) (the MSP web server has commands for processing transaction information associated with the transaction card to obtain authorization from the MSP for the transaction). Initially, as indicated in the Appeal Brief, the Board previously indicated (in the Decision of Appeal of Appeal No. 2004-1809) that col. 9, lines 15-55 of *Muftic* “does not disclose a web server including commands for processing a transaction” (page 3 of the Decision of Appeal; see also pages 2-4 of the Decision of the Appeal).

On page 12 of the Examiner’s Answer, the Examiner posited *Muftic* discloses a web server (“server”) having commands (“programming logic”) for processing transaction information (“business transactions”) associated with the card to obtain authorization (“authorization”) from the MSP (“server”) for the transaction (citing col. 7, lines 16-64; col. 10, lines 27-48; col. 12, line 5 through col. 14, line 62 including col. 13, lines 28-30 of *Muftic*). On page 13 of the Examiner’s Answer, the Examiner further indicated col. 13, lines 28-39 of *Muftic* discloses the web page (“server”) includes commands for processing the transaction information (“order information”). As indicated in the Appeal Brief, these cited portions of *Muftic* do not teach or suggest a web server including commands for processing a

transaction information associated with a card to obtain authorization from a MSP for the transaction as claimed and at least some of these cited portions are generally directed to the same disclosure of col. 9, lines 15-55 of *Muftic*.

In particular, *Muftic* is directed to enabling electronic commercial transactions to be securely conducted over the Internet. To this end, *Muftic* teaches the use of smart token technologies and a public key infrastructure to permit such transactions. (Col. 5, lines 36-41 of *Muftic*.) As a result, electronic payments including credit card numbers may be securely transferred across the Internet. (Col. 6, lines 1-4 of *Muftic*.)

*Muftic* describes “authenticating” transactions conducted over the Internet with the use of public keys and the like in order to securely conduct the transactions. For example, information involved in the transactions which are communicated over the Internet are authenticated as to origin. In this way, users can be authenticated as well as orders and payments of users. (Col. 7, lines 14-64 of *Muftic*.)

Col. 12, line 5 through col. 14, line 62 of *Muftic* includes description of the registration and certification process followed by a user and the operation carried out for conducting transactions after the registration and certification process. The registration and certification process is required so that the user and/or the user’s transactions can be authenticated. In particular, col. 13, lines 28-39 of *Muftic* describes a process for a user to place an order with a vendor after the registration and certification process. The user places an order by logging onto a web server and filling in an order form on a web page of the web server. The user then digitally signs the order form and sends it to the server or directly to the vendor. As such, without more, this section of *Muftic* does not teach or suggest the web server/page including commands for processing transaction information associated with a card to obtain authorization from the MSP for the transaction as claimed as an order form filled out by an authenticated user and digitally signed by the user is transferred to the web server and/or a vendor. This section of *Muftic* further describes that payment may be included during the

order process as discussed “hereinafter” (i.e., col. 13, line 40 through col. 14, line 62 of *Muftic*).

Col. 13, line 40 through col. 14, line 42 of *Muftic* describe payment processes illustrated in FIGS. 11-17 of *Muftic* for including a payment during the order process. FIGS. 13-17 appear to be the most relevant. None of the payment processes are directed to a web server including commands for processing transaction information associated with a card to obtain authorization from a MSP for the transaction as claimed. For instance, col. 14, lines 37-48 of *Muftic* indicates that FIG. 16 illustrates a “Make\_Purchase process using a credit card domain of a smart token”. During this process, the user fills in the electronic ID of a seller and the amount and applies a digital signature. In turn, the electronic charge slip is transferred to the seller. As such, there is no teaching or suggestion of the web server including commands for processing the transaction information to obtain authorization from the seller for the transaction as claimed. Likewise, col. 14, lines 48-62 of *Muftic* indicates the FIG. 17 illustrates a “Make\_CC\_Payment process using a credit card domain of a smart token”. During this process, the user signs a check with a digital signature and the electronic check is transferred to the “issuer’s” computer. It is not clear if the “issuer” is a MSP. In any event, there is no teaching or suggestion of the web server including commands for processing the transaction information to obtain authorization from the issuer for the transaction as claimed.

In summary, the “authentication” of *Muftic* is used to ensure a transaction conducted over the Internet is conducted securely. Presumably, this is to prevent a fraudulent user from posing as a bona fide user during a transaction conducted over the Internet. In contrast, the “authorization” set forth in independent claims 1 and 11-12 is used to ensure that a transaction involving a transaction card is approved by a MSP. Whether the transaction is conducted over the Internet securely or not securely is not at issue.

In view of the foregoing reasons set forth above and in the Appeal Brief, the Applicant respectfully requests the Board reverse the claim rejections set forth in the final Office Action.

Respectfully submitted,

IAN M. DRYSDALE

By:

James N. Kallis  
Registration No. 41,102  
Attorney for Applicant

Date: May 14, 2007

**BROOKS KUSHMAN P.C.**  
1000 Town Center, 22nd Floor  
Southfield, MI 48075-1238  
Phone: 248-358-4400  
Fax: 248-358-3351